The President's National Security Telecommunications Advisory Committee

2003 Research and Development Exchange Breakout Session Briefings

March 14, 2003

The President's National Security Telecommunications Advisory Committee

R&D Exchange
Cyber/Software Breakout Session 1

Mr. Scott Charney, Microsoft
Mr. Phil Lacombe, Veridian

March 14, 2003

Cyber/Software: Current State of Trustworthiness

The group believes that the Office of Science and Technology Policy (OSTP) should focus R&D efforts around three main areas:

- **Short-term research activities that could improve the trustworthiness of software and cyber systems in the near future**
- **Long-term research activities that could embed the concept of trustworthy computing in the design of future systems**
- **Policy issues that either promote or impede the development and deployment of secure and trustworthy cyber systems**

Cyber/Software: Technology To Improve Trustworthiness

Short-term cyber security research priorities should focus on:

- **Economic incentives for developing and deploying secure technologies**
- **Develop methods and tools to eliminate vulnerabilities in the development process**
- **Secure protocol design and development; analyze current routing and signaling protocols**
- **Improving security in legacy systems**
  - **Testing techniques for finding vulnerabilities in existing software and Infrastructures**
  - **Validation and quality assurance of patches**
- **Priority routing in all networks during emergency response with assured quality of service**
  - **Modeling and simulation mechanisms to identify key telecommunications uncovered circuits**
- **System-wide recovery and remediation**
- **Detecting systems' state and developing intelligent systems that measure and monitor incoming/outgoing traffic; configure personal firewall settings automatically; and provide automated policy development, deployment, and enforcement**
- **Understanding what information needs to be shared among infrastructure providers**
- **Promoting risk assessment studies that analyze costs of implementation and consequences of insecurity**
- **Develop a methodology to validate best practices and apply that methodology**

Long-term cyber security research priorities should focus on:

- **Support for basic research in the science of cyber security**
  - **Building and deploying inherently secure architectures**
  - **Testing and evaluation of large scale systems**
  - **Identifying the elements of security**
  - **Defining rules of composition for large scale systems**
  - **Defining and developing technical metrics that measure security and strength of security**
- **Security of embedded systems**
- **Computer security embedded measures to reduce software vulnerabilities**
- **Modeling and simulation of networks**
- **Compilers that eliminate or (at least) find vulnerabilities during compilation**
- **Tools development for authentication, forensics, and attribution**

Cyber/Software: Input to the OSTP and the NSTAC

The group identified a list of vulnerabilities that need to be addressed, which formed the context of our discussion:

- **Internet Signaling Gateway effects on PSN**
- **Signaling and Routing Protocols**
- **Peer-to-peer technology**
- **Trustworthiness of code**
- **Wireless**

The group has also identified promising new technologies:

Network Topology projects:

- **GEWIS (Global Early Warning Internet System) is an early warning system using commercially available/provided global data on internet performance based on industry tools.**
- **CERT is developing a similar network traffic flow program to identify security events.**

R&D cyber security policy recommendations to OSTP:

- **Set the research agenda by focusing on:**
  - **Evolving threats**
  - **Evolving technologies**
  - **The ability to implement the research**
- **Cyber security needs visibility and influence**

The President's National Security Telecommunications Advisory Committee

R&D Exchange
Cyber/Software Breakout Session 2

Carl Landwehr, National Science Foundation
Sami Saydjari, Cyber Defense Agency

March 14, 2003